

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Ming-Shiang Shen

Application No.: 09/478,720

Group No.: 2135

Filed: 01/06/2000

Examiner: Beemnet W. Dada

For: Invention title: Electronic Data Storage Medium With Fingerprint Verification Capability

Mail Stop Petition

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

***SECOND CORRECTED PETITION TO CLAIM BENEFIT UNDER 35 U.S.C. 120 OF
PRIOR FILED NON-PROVISIONAL APPLICATION(S)
(37 C.F.R. § 1.78(a)(2))***

1. The Petitions filed September 19, 2006 and December 19, 2006 contained errors. Applicant hereby corrects that Petition and hereby petitions in accordance with § 1.78(a)(2)(i) to claim the benefit, for this application under 35 U.S.C. 120 of prior application(s):

<u>Application No.</u>	<u>Patent No.</u>	<u>Filed</u>	<u>Granted</u>
09/366,976	6,547,130	August 4, 1999	April 15, 2003

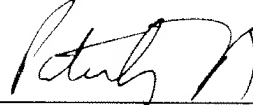
2. Applicant states that the entire delay between the date the claim for the benefit of the earlier application was due under paragraph (a)(2)(ii) of 37 C.F.R. § 1.78 and the date this claim is filed was unintentional.
3. **A Substitute Amendment entering the reference required by 35 U.S.C 120 and 37 C.F.R. 1.78(a)(2)(i) is submitted herewith.** Applicant's attorney was not sure how to comply with the requirement raised in the Decision on Petition mailed July 13, 2007, and was unable to contact Petitions Attorney Brown after several tries to clarify how the correction was to be made. Applicant's attorney interpreted in good faith the paragraph in the middle of page 2 of the Decision as requiring (a) this corrected petition, and (b) the attached Substitute Amendment, which is intended to replace the last-filed Amendment, which was originally filed on June 8, 2006.

4. **The surcharge fee set forth in § 1.17(t) (\$1,370.00), required by 37 C.F.R. 1.78(a)(3)(ii), has already been charged to our American Express card on 9/19/2006. Enclosed is Exhibit A showing the transaction.**

If any additional fees are due, authorization is hereby made to charge Deposit Account No. 50-0574.

Date: July 23, 2007

Reg. No.: 33834
Tel. No.: 1-408-451-5902
Customer No.: 22888



Signature of Practitioner
Patrick T. Bever
Bever, Hoffman & Harms, LLP
2099 Gateway Place, Suite 320
San Jose, CA 95110

Transaction Details

[Learn how to dispute a charge](#)

[Print Window](#)

[Close Window](#)

Business Gold Card - 71029 Transaction Detail

Transaction Date:	09/19/2006
Post Date:	No Additional Information
Transaction Description:	US PATENT TRADEMARK 571-2726500 VA GOVERNMENT SERVICES ROC No. 9246
Charge:	\$1,370.00
Merchant Address:	US PAT/TRADEMARK SYS COPY CRYSTAL PARK 1 ROOM 802 WASHINGTON DC 20231 USA
Merchant Type:	FED ST MUNCPL GOVT
Doing Business As:	US PATENT TRADEMARK

[Back to Top](#)

EXHIBIT A

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Ming-Shiang Shen

Assignee: Super Talent Electronics, Inc.

Title: ELECTRONIC DATA STORAGE MEDIUM WIT FINGERPRINT
VERIFICATION CAPABILITY

Serial No.: 09/478,720-2064 File Date: January 6, 2000

Examiner: Beemnet W. Dada Art Unit: 2135

Docket No.: SUP-029 (STI-102)

July 23, 2007

Mail Stop Petition
Commissioner of Patents
P.O. Box 1450
Alexandra, VA 22313-1450

SUBSTITUTE AMENDMENT IN RESPONSE TO FINAL OFFICE ACTION

Dear Sir:

This Substitute Amendment is intended to replace the Amendment dated June 8, 2006, which was filed in response to the Office Action dated June 16, 2004--please amend the above-identified application as follows.

IN THE SPECIFICATION

Please amend page 1 of the specification to include the following on line 3 (between the second line of the title and the heading "BACKGROUND OF THE INVENTION":

Related Applications

This application is a continuation-in-part of Application No. 09/366,976, filed August 4, 1999, now U.S. Patent No. 6,547,130.

IN THE CLAIMS

Please amend the claims as follows:

1. (currently amended) An electronic data storage medium adapted to be accessed by a data terminal, said electronic data storage medium comprising:

a non-volatile memory device for storing a data file and fingerprint reference data obtained by scanning a fingerprint of a person authorized to access the data file;

a fingerprint sensor adapted to scan a fingerprint of a user of said electronic data storage medium and to generate fingerprint scan data;

an input/output interface circuit activable so as to establish communication with the data terminal; ~~and~~

a processing unit connected to said non-volatile memory device, said fingerprint sensor and said input/output interface circuit,

means for controlling said processing unit ~~being operable selectively~~ in a programming mode, where said processing unit activates said input/output interface circuit to receive the data file and the fingerprint reference data from the data terminal, and to store the data file and the fingerprint reference data in said non-volatile memory device, and

means for controlling said processing unit in a data retrieving mode, which is performed subsequent to the programming mode, where said processing unit receives the fingerprint scan data from said fingerprint sensor, compares the fingerprint scan data with the fingerprint reference data in said non-volatile memory device to verify if the user of said electronic data storage medium is authorized to access the data file stored in said non-volatile memory device, and activates said input/output

interface circuit to transmit the data file to the data terminal upon verifying that the user of said electronic data storage medium is authorized to access the data file stored in said non-volatile memory device.

2. (currently amended) The electronic data storage medium of Claim 1, further comprising a card body on which said non-volatile memory device, said fingerprint sensor, said input/output interface circuit and said processing unit are mounted.

3. (original) The electronic data storage medium of Claim 2, further comprising a power source mounted on said card body and connected to said processing unit for supplying electrical power thereto.

4. (currently amended) The electronic data storage medium of Claim 1, wherein said non-volatile memory device is a flash memory device.

5. (currently amended) The electronic data storage medium of Claim 1, wherein said processing unit stores the data file and the fingerprint reference data in said non-volatile memory device in a compressed format.

6. (original) The electronic data storage medium of Claim 1, further comprising a function key set connected to said processing unit and operable so as to initiate operation of said processing unit in a selected one of the programming and data retrieving modes.

7. (currently amended) The electronic data storage medium of Claim 1, wherein said processing unit is further operable selectively in a data resetting mode, where the data file and the fingerprint reference data are erased from said non-volatile memory device.

8. (original) The electronic data storage medium of Claim of 7, further comprising a function key set connected to said processing unit and operable so as to initiate operation of said processing unit in a selected one of the programming, data retrieving and data resetting modes.

9. (original) The electronic data storage medium of Claim 8, wherein said memory device further stores a reference password therein, said function key set being operable to provide an input password to said processing unit, said processing unit comparing the input password with the reference password and initiating operation in the data resetting mode upon verifying that the input password corresponds with the reference password.

10. (currently amended) The electronic data storage medium of Claim 7, wherein said processing unit automatically initiates operation in the data resetting mode upon detecting that a preset time period has elapsed since storage of the data file and the fingerprint reference data in said non-volatile memory device.

11. (original) The electronic data storage medium of Claim 1, further comprising a display unit connected to and controlled by said processing unit for showing the data file exchanged with the data terminal thereon.

12. (New) An electronic data storage medium adapted to be accessed by a data terminal, said electronic data storage medium comprising:

a non-volatile memory device for storing a data file and fingerprint reference data;

a fingerprint sensor adapted to scan a fingerprint of a user of said electronic data storage medium and to generate fingerprint scan data;

an input/output interface circuit for establishing communication with the data terminal;

a processing unit coupled to said non-volatile memory device, said fingertip sensor and said input/output interface circuit;

a function key set connected to said processing unit and operably arranged such that a user is enabled to initiate operation of said electronic data storage medium in a selected one of a programming mode and a data retrieving mode by manipulation of the function key set;

means for controlling said processing unit when the electronic data storage medium is in the programming mode such that the processing unit writes at least one of the data file and the fingerprint reference data into said non-volatile memory device; and

means for controlling said processing unit when the electronic data storage medium is in the data retrieving mode such that the processing unit compares the fingerprint scan data entered through said fingerprint sensor with the fingerprint reference data stored in said non-volatile memory device, and transmits the data file through said input/output interface circuit to the data terminal only

when the fingerprint scan data matches the fingerprint reference data.

13. (new) The electronic data storage medium of Claim 12,

wherein said non-volatile memory device further comprises means for storing a reference password therein, and

wherein said function key set includes means for transmitting an input password manually entered by a user to said processing unit,

and wherein the electronic data storage medium further comprises means for controlling said processing unit to compare the input password with the reference password and initiating operation in the data resetting mode upon verifying that the input password corresponds with the reference password.

14. (New) An electronic data storage medium adapted to be accessed by a data terminal, said electronic data storage medium comprising:

a non-volatile memory device for storing a data file and reference data possessed by a person authorized to access the data file;

security means for entering the security data into the electronic data storage medium;

an input/output interface circuit for establishing communication with the data terminal;

a processing unit coupled to said non-volatile memory device, said security means and said input/output interface circuit;

means for manually switching the electronic data storage medium between a programming mode and a data retrieving mode;

means for controlling said processing unit when the electronic data storage medium is in the programming mode such that the processing unit transfers at least one of the data file and the reference data from the input/output interface circuit into said non-volatile memory device, and

means for controlling said processing unit when the electronic data storage medium is in the data retrieving mode such that the processing unit compares the security data entered through said security means with the reference data stored in said non-volatile memory device, and activates said input/output interface circuit to transmit the data file to the data terminal only when the security data matches the reference data.

REMARKS

This Substitute Amendment is responsive to the Decision on Petition dated July 13, 2007, and enters the relationship between the present application and prior filed application No. 09/366,976.

The contents of the original Amendment, contained herein, are responsive to the Office Action mailed from the Patent and Trademark Office on June 16, 2004, which has a shortened statutory period set to expire September 16, 2004. A petition to revive the application is submitted in a paper filed with the original Amendment.

Claims 1-11 are pending in the above-identified application. Claims 1, 2, 5, 6 and 11 are rejected under 35 USC 102, and Claims 3 and 7-10 are rejected under 35 USC 103.

In the current paper, Claims 1, 2, 4, 5, 7 and 10 are amended, and Claims 12-14 are newly entered. No new matter is entered. In view of these amendments and the following remarks, Applicants respectfully request reconsideration and withdrawal of all pending rejections.

Rejections Under 35 USC 102

Claims 1, 2, 5, 6 and 11 are rejected under 35 USC 102(e) as being anticipated by Bjorn (U.S. Patent No. 6,125,192).

Claim 1 is amended herein to recite (in pertinent part) "a non-volatile memory device". Support for this limitation is provided, for example, in original Claim 4, which recites that the memory device is a "flash" memory device. Those skilled in the art recognize that a flash memory device represents one type of non-volatile memory device.

Claim 1 is also amended to incorporate "means for" type claim language that sets forth the functions performed by the processing unit recite in arguably a more appropriate manner. No new matter is entered by this amendment.

Finally, Claim 1 is amended to clarify that the "data retrieving mode ... is performed subsequent to the programming mode". Support for this amendment is found, for example, on pages 4 and 5 of Applicant's specification.

No new matter is entered by the above-mentioned amendments.

As amended, Claim 1 recites an electronic data storage medium that is suitable for securely storing personal "data file" information (e.g., a credit card number, a bank account number, or an assigned user identification card number), and for only passing the information to a host system when the electronic data storage medium verifies that the authorized user is present by way of matching a scanned fingerprint with a previously stored fingerprint. The electronic data storage medium therefore includes a "non-volatile [e.g., flash] memory device for storing a data file and fingerprint reference data", both of which being stored during a "programming mode". During a "data retrieving mode" performed subsequent to the "programming mode", "fingerprint scan data" received from a "fingerprint sensor" is compared with the previously-stored fingerprint reference data, thereby allowing the owner of the electronic data storage medium to maintain security control over the stored fingerprint reference data.

In contrast to the electronic data storage medium recited in Applicants' Claim 1, Bjorn teaches a Fingerprint recognition system in which a portion of

a scanned fingerprint is transmitted to a host system for preliminary identification (i.e., matching with a fingerprint stored in a database of templates), and then the "preliminary match" is transmitted back to the "sensor" for "final matching". This process is described with reference to Column 8, line 44 to Column 9, line 12 and Figs. 6A and 6B, which are copied below for reference:

8

At block 625, a nonce is sent to the sensor 250. The nonce includes a time/date stamp, the current session key, and other information. It is used to verify the identity of the sensor as well as the currency of the fingerprint.

At block 630, a differential print is received from the sensor 250. This, once again, may be an interrupt. The hash is a combination of the nonce, and the differential print, as described above. At block 635, the hash is decoded, and the nonce is verified. Additionally, the session key may be verified.

At block 640, the differential print is compared to a database of templates. The database of templates includes all users who are registered with this system. The received print is compared to prints in the database. Such methods are known in the art. Processing continues at block A shown in FIG. 6B.

Referring to FIG. 6B, at block 645, the process of the present invention tests whether a preliminary match was found. If no match was found, the process continues directly to block 670. If the preliminary match was found, the process continues to block 650, and both the match and the hash are returned to the sensor for final matching. This is necessary if the digital system, in which actual analysis is done, is not secure. By returning the print and match

9

characteristics to the sensor, the process can be made secure. Alternatively, the final match may be done in the digital system 210.

At block 655, a verifying match/no match signal is received from the sensor. Because the sensor is a closed and secure system, the final decision, regarding whether a match was found or not, is left to the sensor. In this way, possible tampering with the digital system 210 does not result in a false positive signal.

At block 660, it is determined whether the final answer is a yes or a no, i.e. whether the prints match or do not match. If the prints do not match, at block 670, access is refused.

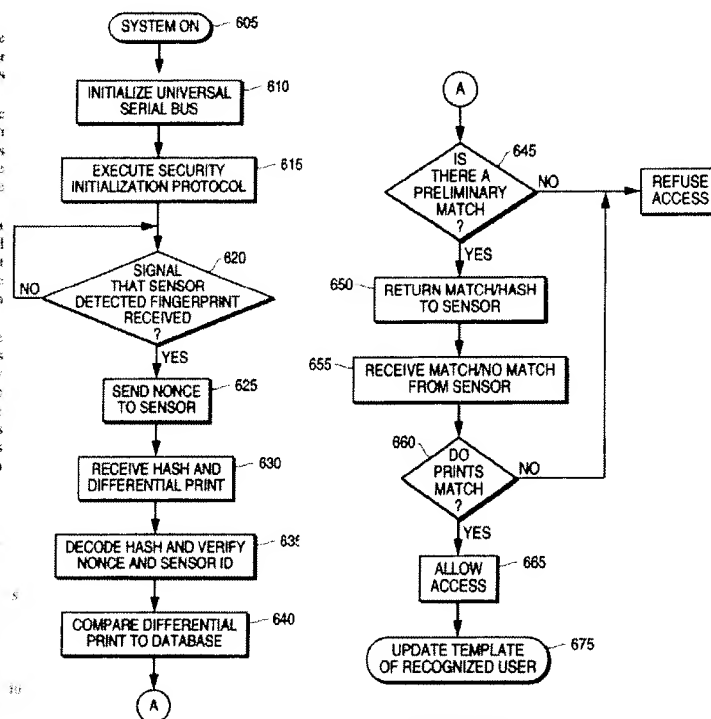


FIG. 6A

FIG. 6B

As recognized by the Examiner in the pending rejection directed to Claim 1 under 35 USC 102, Bjorn fails to teach the storage of fingerprint reference data in a "non-volatile memory device" as recited in Claim 1. Based on the description of Bjorn's system (copied above), Applicant contends that it would not have been obvious to provide either a "non-volatile memory" or "means for controlling said processing using ... to store ... the fingerprint

reference data in said non-volatile memory device" on an electronic data storage medium that includes Bjorn's fingerprint recognition system because the "match" found in Bjorn's step 645 is written from a host system to the sensor in step 650 during each fingerprint recognition process (see Col. 8, lines 63-65, copied above). That is, because the "match" is written during each fingerprint recognition process, there is no reason to store the "match" for longer than the time it takes to perform the comparison associated with Bjorn's step 660. For this reason, Bjorn in effect teaches away from providing an electronic data storage medium that includes Bjorn's fingerprint recognition system with "non-volatile memory" and "means for controlling said processing unit in a programming mode ... to store ... the fingerprint reference data in said non-volatile memory device", as recited in Claim 1. Hence, the owner of an electronic data storage medium that includes Bjorn's fingerprint recognition system would not have control over the information stored on the card, thus making the electronic data storage medium unsuitable for, for example, making credit card purchases in stores that do not have access to the "database of templates".

Claims 2, 4, 5, 7 and 10 are amended to be consistent with the amendments entered in Claim 1 (discussed above).

Claims 2, 5, 6 and 11 are dependent from Claim 1, and are therefore distinguished over Bjorn for at least the reasons provided above with reference to Claim 1.

For the above reasons, Applicants' respectfully request reconsideration and withdrawal of the rejections under 35 USC 102.

Rejections Under 35 USC 103

Claims 3 and 7-10 are rejected under 35 USC 103(a) as being unpatentable over Bjorn in view of Jacobsen et al (U.S. Pub. App. No. 2001/0043174).

Claims 3 and 7-10 are dependent from Claim 1, which is distinguished over Bjorn for at least the reasons provided above. Further, Jacobsen fails to overcome the deficiencies of Bjorn that are described above with reference to Claim 1. Hence, it would have been neither possible nor obvious to combine the teachings of Jacobsen and Bjorn to produce the electronic data storage medium recited in Claim 1. Because Claims 3 and 7-10 are dependent from Claim 1, they are believed to be patentable over Bjorn and Jacobsen for at least this reason.

For the above reasons, Applicants' respectfully request reconsideration and withdrawal of the rejections under 35 USC 103.

New Claims

Claims 12-14 are newly entered.

Similar to Claim 1, Claim 12 recites a "non-volatile memory device", a "fingerprint sensor", an "input/output interface circuit", a "processing unit", "means for controlling said processing unit when the electronic data storage medium is in the programming mode" and "means for controlling said processing unit when the electronic data

storage medium is in the data retrieving mode". As such, Claim 12 is believed to be distinguished over Bjorn and Jacobsen for reasons similar to those provided above with reference to Claim 1.

In addition, Claim 12 recites "a function key set connected to said processing unit and operably arranged such that a user is enabled to initiate operation of said electronic data storage medium in a selected one of a programming mode and a data retrieving mode by manipulation of the function key set". Support for this amendment is found, for example, on page 5, lines 18-27. The recited "function key" further enhances control of the electronic data storage medium by controlling writing to the non-volatile memory only during the "programming mode". As discussed above, Bjorn's fingerprint recognition system does not involve storing fingerprint reference data in a non-volatile memory of an electronic data storage medium, thus obviating the need for operation in a "programming mode" for this purpose. As such, it would not have been obvious to modify the teachings of Bjorn to include the "function key set" recited in Claim 12.

Claim 13 is dependent from Claim 12, and is therefore distinguished over the cited prior art for reasons similar to those provided above with reference to Claim 12.

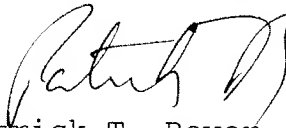
Similar to Claim 1, Claim 14 recites a "non-volatile memory device", an "input/output interface circuit", a "processing unit", "means for controlling said processing unit when the electronic data storage medium is in the programming mode" and "means for controlling said processing unit when the electronic data storage medium is in the data retrieving mode". As such, Claim 14 is

believed to be distinguished over Bjorn and Jacobsen for reasons similar to those provided above with reference to Claim 1. Claim 14 also recites "means for manually switching the electronic data storage medium between a programming mode and a data retrieving mode" in a manner similar to that recited above with reference to Claim 12, thus further distinguishing Claim 14 over the teachings of Bjorn and Jacobsen. Note that Claim 14 also recites "security means" that are enabled, for example, by the fingerprint sensor and/or function key set disclosed in Applicant's specification.

CONCLUSION

For the above reasons, Applicants believe Claims 1-14 are believed to be in condition for allowance. Should the Examiner have any questions regarding the present paper, the Examiner is invited to contact the undersigned attorney at the number provided below.

Respectfully submitted,



Patrick T. Bever
Attorney for Applicant
Reg. No. 33,834
408-451-5902

Customer No.: 22888